indicators of fraudulent use. Some of the steps/options that a PBX owner may take to protect its equipment from fraudulent intrusion include:

1. Do not activate the remote access features;
2. Install a traffic counter to count the number of calls that utilize the remote access feature. Contemporaneous reports may alert or notify local management of unusual use of the feature (including nights and weekends);
3. Regularly disable and reissue personal identification numbers;
4. Use long (8 to 10 digit) personal identification numbers rather than easily compromised 4-digit numbers;
5. Require PBX users to go through a console with an attendant to use remote access long distance features;
6. Set PBX to let a line ring 6 or 7 times before a second dial tone is provided. Most hackers using an auto dialer abandon a number after 3 rings. The PBX should not automatically return internal dial tone;
7. Require a second barrier and PIN before outgoing dial tone is provided;
8. Create multiple barriers requiring different PINs for each barrier;
9. Use audit trails to track calls placed through the remote access unit;
10. Program PBX to limit remote access feature during the times when legitimate traffic is not anticipated;
11. Order outgoing lines with restrictions — e.g. continental US only, no operator access, international calls require console intervention;
12. Block access to tie lines to other PBX units;

13. Block access to WATS lines either entirely or by use of a second code;
14. Use a traffic counter to detect attack by hackers. Set a threshold of a certain number of invalid PIN attempts within a specified time and activate an alert or report or even disable the remote access unit until it is reset by an individual with proper authorization;
15. Employ a token access device such as an access card. The access card displays a Personal Identification Number. The PBX and the access card are programmed to change the PIN simultaneously every few moments, at which time a new PIN appears on the access card.
16. Manage the system daily to analyse call volumes, length, destinations, and timing of calls;
17. Disconnect or restrict modems and ports at the PBX that are used by the vendor for upgrades or repairs.

VII. Industry Efforts

Several industry forums, such as the Toll Fraud Prevention Committee (TFPC) and the Communications Fraud Control Association, meet to consider and resolve issues involving telecommunications fraud. Other organizations such as the North American Telecommunications Association (NATA), also deal with issues such as PBX toll fraud, equipment vulnerabilities and safeguards, system management skills, etc. Each of these bodies can assist in the education process.

NYT, through its NYNEX representative to the Toll Fraud Prevention Committee, has proposed the subject of PBX remote access fraud as an issue for consideration by that forum. While the TFPC does not set standards for

central office or PBX equipment manufacturers, it can influence its membership (LECs, IXCs, enforcement agencies) to take steps that will further reduce the industry's vulnerability to fraud. NYT believes that discussion of the PBX toll fraud issue in such forums will help to generate solutions to aid the PBX user.

VII. Conclusion

Mr. Chairman, New York Telephone is very willing to do its part to help reduce and eliminate toll fraud. But as you can see from my testimony, we are limited in the role we can play in solving this serious problem. We believe that the first and primary line of defense against remote access PBX toll abuse is prevention, and the primary responsibility and capability for prevention lies with educated PBX users. The second line of defense - real time detection of fraud in progress - is within the capacity of the PBX owner and the interexchange carriers. The new services recently announced by some interexchange carriers to limit the effects of toll fraud are examples of effective detection plans. The third line of defense is identification of the incidence of fraud after it has taken place. NYT's Advance Toll Notifier procedures, for example, provide this ability on a limited basis.

The customer who wants the convenience and the potential savings available through use of the remote access and other features subject to fraud, should also manage its PBX to minimize fraudulent opportunities. PBX manufacturers play a crucial role by providing management features to PBX users and by educating their customers. The PBX owner best knows the criteria

of legitimate calls. The PBX itself is the best place to control and measure and restrict PBX usage. In addition, the interexchange carrier handling the interLATA and international calls originating through the PBX can control, measure and restrict such calls. NYT is glad to work with PBX customers, manufacturers, IXCs and law enforcement agencies in an attempt to help reduce and eliminate toll fraud.

Mr. Chairman, on behalf of New York Telephone and our customers who have suffered from toll fraud, thank you for your interest and for allowing me this time to address your committee.

New York Telephone
A NYNEX Company
1095 Avenue of the Americas
New York, New York 10036

July 2, 1992

The Honorable Edward Markey
Chairman
Subcommittee on Telecommunications and Finance
Committee on Energy and Commerce
House Annex II, Rm 316
Washington, DC 20515

Dear Chairman Markey:

Attached are my responses to the follow-up questions associated with the toll fraud hearing held June 11, 1992, as requested in your correspondence to me dated June 22, 1992. Please do not hesitate to cantact me on (212) 395-0505 or Sue Browning in our Washington office on (202) 416-0123 if you need any additional information on these issues.

Sincerely,

Jane Gracalone

cc: Myron Sagall

Attachment

FOLLOW-UP QUESTIONS FOR NYNEX

QUESTION NO. 1:

Please reference New York Telephone petition before the FCC (attached) dated April 18, 1990, in the matter of: "Compliance With Opinion No. 90-13 of the New York Public Service Commission in Case 88-C-102 Regarding Blocking of InterLATA 1+ and 10XXX+1 Dialed Calls." Page 4, footnote 5 indicates certain types of call blocking (alluded to above) can "be made available at relatively minor cost (less than $1 million rather than in excess of $100 million)" in various switches within six months. Extrapolating from that capability, would it not be possible to extend this service to international call blocking? If not, why not?

RESPONSE TO QUESTION NO. 1:

The ability of NYT to perform blocking at the central office is dependent on the type of blocking desired and the switch technology. NYT does perform certain blocking functions today under tariff, but as described below, these functions are significantly different than the international blocking proposed at the hearing on June 11, 1992.

The blocking referred to in NYPSC (New York Public Service Commission) Case 88-C-102 blocks at the central office switch all normally dialed interLATA 1+ and interLATA 10XXX+1 calls (both domestic and international while permitting interLATA 0+ and 10XXX+0+ dialing.). The NYPSC forced this feature on COCOT (customer owned coin operated pay telephones) and AOS (Alternate Operator Service) vendors to minimize widespread fraudulent calls on these lines while permitting the public to make operator assisted calls with their interexchange carrier of choice. The COCOT providers may accomplish the blocking through their own public telephone sets, or by using a feature NYT was ordered to provide in those switches where technically possible.

This blocking feature currently offered by NYT (interLATA 1+ and 10XXX+1 blocking) does not appear to address the concerns of PBX owners or other business customers because it blocks all interLATA calls made on a direct-dialed basis (i.e., normal 1+ as well as 10XXX+1 dialed calls). Thus, a call from a New York City business using the feature that desired to reach New Jersey or Connecticut would have to be made as an operator assisted call (i.e., 0+) at operator assisted rates. Such calls cost more than normal 1+ dialed calls. Few, if any business customers would want to pay operator-assisted rates on each and every interLATA call. New York Telephone is not aware of any business customer asking for such blocking. Additionally, the feature is basically available only in NYT's 5ESS, 1 ESS and DMS-100 switches.

If a business customer wanted calling to all international locations blocked at the local switch, NYT would need to make major routing and translation changes that are significantly different and more complex than the interLATA restrictions in place for AOS customers. Potentially additional memory and other equipment would be required in some central offices. Very preliminary estimates indicate deployment of such a service in central offices where possible would cost in excess of $10 million. It should be noted that selective blocking within the 809 NPA would require even more extensive programming and call processing changes.

More sophisticated blocking options, such as blocking individual lines for selective international locations, would appear to be a more probable request from business customers. The feasibility of complying with such a request would need to be evaluated on a case by case basis. It would be dependent on the type of switching equipment in the central office from which the customer is served. Some offices have limitations that would prevent the technical offering of such requests. Each switch would need to be evaluated for the feasibility of such a feature, the memory required, the interaction with other features, and the downstream repair and billing system impacts. As a general rule, line by line restrictions are much more costly than the generic class of service blocking done by NYT for COCOTs lines.

Even if customer specific international blocking service were evaluated, found feasible and implemented at rates to cover the cost of the service, there is still a question of the effectiveness of such a service. If a defrauder retained the ability to enter the interexchange carrier's network by first dialing a domestic call, and then "sequencing" the calls, the screening in the local carrier switch would have no impact on any subsequent international calls made in the interexchange carriers network, since the customer would be directly connected to the interexchange carrier, not to the local carrier.

Another possibility to accomplish international blocking would be to block <u>all</u> direct dialed international calling within a central office and require all customers (business, residence, government, etc.) served by the central office to use interexchange carriers' operators. This option would be technically feasible for NYT, but would cause a severe degradation of service for customers needing to make legitimate international calls and desiring the lower prices for direct dialed calls.

The PBX owner can implement effective restrictions, including the elimination of international access entirely, by utilizing software applications. Approaching the blocking directly by using features within the PBX allows each PBX customer the flexibility to meet its unique business needs. The recent announcement that NYT is blocking international calls from selected public phones at Times Square and other locations in midtown Manhattan to help long distance carriers crack down on rampant telephone fraud is being accomplished through the public telephone set, not through the local central office switch.

QUESTION NO. 2:

Please reference the attached C&P Telephone letter, dated June 25, 1990, addressed to the PSC of Maryland, which describes an overseas call blocking option. If this capability is available to one of the BOCs, why is this service not available to NYNEX?

RESPONSE TO QUESTION NO. 2:

C&P Telephone Company's offering of an Overseas Call Blocking service to its COCOTs customers, whereby directly-dialed international calls (i.e., calls dialed 011+ and 10XXX+011+) are blocked, is already offered by New York Telephone Company to its COCOTs customers, although in a somewhat different form pursuant to an order of the New York State Public Service Commission. NYT's LIDPAL (Limited InterLATA Dialing for Public Access Lines) offering to COCOT customers blocks all interLATA directly-dialed calls not requiring operator assistance (i.e., 1+, 10XXX+1+, 011+ and 10XXX+011+). (See response to Question No. 1.)

As with C&P, NYT's blocking is not available in all offices, and is available only to COCOT (and AOS) vendors. There has been no market demand for a feature blocking all interLATA directly dialed calls from other types of lines.

QUESTION NO. 3:

Does NYNEX have any policy, either formal or ad hoc, to reduce inter-exchange carrier access charges where the calls made were fraudulent? Has NYNEX discussed this possibility with any IXC?

RESPONSE TO QUESTION NO. 3:

NYT has no formal policy to reduce inter-exchange carrier access charges where the calls made were fraudulent. From time to time, however, NYT has settled disputes with inter-exchange carriers regarding liability for fraudulent calls; pursuant to those settlements, NYT has made payments to carriers. NYNEX has had discussions with inter-exchange carriers regarding the possibility of reducing carrier access charges for certain types of fraudulent calls, e.g. calling card calls.

ATTACHMENT C

May 14, 1992
TFPC

Subscription Fraud
(External)

It's a billion-dollar-a year business that's getting bigger every year. The United States Secret Service estimates that telecommunications fraud exceeded $1.2 billion in 1991.

Consumers in every state are paying more than they need to because of fraud and the issue is of legitimate concern to regulators, local and long distance companies alike.

Only through the concerted efforts of everyone affected by fraud will its costly impact be reduced, if not eliminated.

There are many types of telecommunications fraud; one of the most pernicious is Subscription Fraud.

A legitimate question to ask is: If the industry is aware of the problem, why doesn't it establish procedures to eliminate the fraud? And the answer is: Many procedures are in place to identify and prevent potential fraud, but more weapons are needed to successfully combat those who conspire to defraud local and long distance companies.

In some cases, regulatory guidelines designed to promote universal service frequently enable the person intent on fraud to gain access to the network with a minimum of verifiable references. Long distance companies, which frequently suffer the largest loss from fraud, do not have any input prior to a subscriber signing up for their service. Rather, they are notified of their selection after the fact. The fraud, however, begins immediately.

Calls are made to and bridged between countries that have no direct communication links, such as the Middle East. Calls from restricted telephones such as prison telephones or coin telephones are accepted "collect" and then relayed to distant points.

In transportation centers or on street corners, fraudulent "call sell" operations are established. A local telephone operator, when checking for authorization to bill a call to the account, will receive positive, but fraudulent, acceptance. Losses of $20,000 to $30,000 in a single day have been generated.

What can be done to correct this vulnerability, to protect the consumers who ultimately pick up the tab? There are no easy answers, but each party can play a significant role: the local telephone company, the long distance company, state and federal regulators, legislators and consumers.

The local telephone company is the first point of contact, where the network connection is made. While it might seem easy to keep fraudulent customers off the network, it is difficult in practice. Local telephone companies can improve their effectiveness by following these steps:

- **Initial Service Request** - Local telephone company representatives should be aware of the typical profile of an account set up for subscription fraud.

- **Installation Service** - Installation technicians can provide excellent intelligence before fraud starts. Virtually every location requires on-site work, since multiple lines are ordered. The installer also will be one who can identify anyone on the premise should an arrest occur.
- **Customer Service** - Telephone accounting systems frequently use billing thresholds called high toll notifiers. The local telephone company should evaluate the feasibility of developing programs to improve early detection. Further investigation would be necessary to demonstrate whether or not fraud has been committed. Moreover, where special billing and collection contracts exist between local telephone and long distance companies, additional steps can be developed.
- **Security Department**- The privacy of communications is a guiding principle for local telephone companies and there are well defined procedures and regulations on what can be done in pursuing leads or divulging findings to external parties. The operations of the local telephone company's Security Department properly allow for the detection of billing evasion schemes, including accumulation of data that can be used in a court of law. Consequently, security managers should work closely with their internal coordinates to investigate suspect accounts.
- **Product Development** - Data base services which support alternate billing services can be enhanced to offer added protection. Thresholds to count collect and bill to third number attempts can be deployed. New products and services should be analyzed for fraud implications prior to deployment. Enhancements to billing systems should facilitate the identification and tracking of fraud losses.

Long distance companies have an incentive to identify subscription fraud. A long distance company that protects its own network (e.g., by blocking calls from a problem telephone line) can help protect the industry as well. The long distance company can work cooperatively with the local telephone company through their respective security departments. In that way, efforts to investigate accounts, document any abuse, and shut down the fraud) including involvement of the appropriate law enforcement agencies) will help prevent its migrating to another company.

Where a contract for billing exists between the long distance and local telephone companies, the long distance company should arrange to accelerate delivery of billing tapes. Delivery at long intervals (e.g., every 30 days) virtually eliminates the value of the local telephone company's high toll notifier systems. Rather, such delays make it likely that a long distance company will be victimized by defrauders.

Regulators need to recognize and support the industry's growing need to reduce telecommunications fraud. Losses are not always easily quantified and may not appear to impact state residents (e.g., international calls are under interstate jurisdiction). Nevertheless, losses are enormous in the aggregate, and significant harm is done in the local market. The long distance companies recover these losses from legitimate callers. The local telephone company must also recover its administrative expenses (negotiation, installation, investigation, disconnection, adjustments, etc.), as well as losses from line rentals and local usage.

Regulators' concerns about nondiscrimination and privacy are shared by all. However, regulators need to permit the local telephone company sufficient flexibility--when negotiating new service--to take legitimate precautions to protect itself, its rate payers, and indeed, even the industry. This may include requiring positive identification from applications. Some greater latitude is also appropriate when the telephone company suspects that fraud will likely generate large uncollectibles, as with Subscription Fraud. Timely pre-billing corrective action should take place so that losses do not escalate, while, for example, written warnings of suspension are mailed.

Telephone customers can play an important role by reporting incidents of suspected fraud to their local telephone company business offices. Caution is appropriate, and their timely referrals are appreciated.

Subscription Fraud--and all telecommunications fraud--penalizes each consumer, the industry, and the whole economy. No one segment of the industry can combat fraud effectively, but concerted action can change the trend line of mushrooming losses. Above all, flexibility and speedy cooperation are needed. One must remember that fraud is big business, and the returns are dramatic. One can expect that the defrauders will be as imaginative and resilient in the future as they have been in the past. So must be those who will battle telecommunications fraud.